A NEW APPROACH TO ENHANCE SECURITY AGAINST MALICIOUS NODES USING KD2SA

D.Abinaya[1], Mr.B.Senthilmurugan[2]
[1]PG Scholar, Dept of ECE, [2]Assistant Professor/ECE/M.E
Thanthai Periyar Government Institute of Technology, Vellore, Tamil Nadu, India

ABSTRACT: In MANET (Mobile AdHoc Network), a primary requirement for the establishment of communication among nodes is that nodes should cooperate with each other. The proposed mechanism adaptive dynamic routing is presented that effectively detects the malicious nodes that attempt to launch Wormhole attacks. In our scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a modified reverse tracing technique. Any detected malicious node is kept in a wormhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of adaptive dynamic routing lies in the fact that it integrates the proactive and reactive defense architectures to achieve the mentioned goal.

KEYWORDS: Packet Drop, Energy Gain, Worm hole, Black hole

I. INTRODUCTION

Sensor networks are a special category of ad hoc wireless networks that are used to provide a wireless communication infrastructure among the sensors deployed in a specific domain. Sensor nodes are tiny devices that sense the physical parameters, process the data gathered and communicate over the network to the monitoring station. The activity of sensing can be periodic or sporadic. The factors like mobility of the nodes, size of the network, density of deployment, power constraints, and traffic distribution makes sensor networks a distinct category of ad hoc wireless networks. Sensor nodes are expected to operate in harsh environmental or geographical conditions with minimum or no human supervision and maintenance. In certain cases, recharging of energy source is impossible. Power sources used in sensor networks can be classified as replenish able, non-replenish able and regeneratable power sources.

The term MANET (Mobile Ad hoc Network) refers to a multi hop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure. MANET is actually self-organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. A MANET is a type of ad hoc network that can change locations and configure itself on the fly. Because MANETS are mobile, they use wireless connections to connect to various networks. This can be a standard Wi-Fi connection, or another medium, such as a cellular or satellite transmission

Figure 1 Structure of mobile computing

II. RELATED WORK

Many research works have investigated the problem of malicious node detection in MANETs. Most of these solutions deal with the detection of a single malicious node or require enormous resource in terms of time and cost fordetecting cooperative blackhole attacks. In addition, some of these methods require specific environments or assumptions in order to operate. In general, detection mechanisms that have been proposed so far can be grouped into two broad categories. Proactive detection schemes are schemes that need to constantly detect or monitor nearby nodes. In these schemes, are those that trigger only when the destination node detects a significant drop in the packet delivery ratio. Among the above schemes are the ones proposed in and which we considered as benchmark schemes for performance comparison purposes. In Liu et al. proposed a 2ACK scheme for the detection of routing misbehavior in MANETs. In this scheme, two-hop acknowledgement packets are sent in the opposite direction of the routing path to indicate that the data packets have been successfully received. A parameter acknowledgment ratio, i.e., Rack, is also used to control the ratio of the received data packets for which the acknowledgment is required. This scheme belongs to the class of proactive schemes and, hence produces additional routing overhead regardless of the existence of malicious nodes. Nahrstedt proposed a prevention mechanism called best-effort fault-tolerant routing (BFTR). Their BFTR scheme uses end-to- end acknowledgements to monitor the quality of the routing path (measured in terms of packet delivery ratio and delay) to be chosen by the destination node. If the behavior of the path deviates from a predefined behavior set for determining “good” routes, the source node uses a new route. One of the drawbacks of BFTR is that malicious nodes may still exist in the new chosen route, and this scheme is prone to repeated route discovery processes, which may lead to significant routing overhead. Our proposed detection scheme takes advantage of the characteristics of both the reactive and proactive schemes to design a DSR-based routing scheme able to detect grayhole/collaborative blackhole attacks in MANETs.

III. EXISTING METHODOLOGY

In the Existing system a detection scheme called the cooperative bait detection scheme (CBDS), which aims at detecting and preventing malicious nodes launching grayhole/collaborative blackhole attacks in MANETs. In our approach, the source node stochastically selects an adjacent node with which to cooperate, in the sense that the address of this node is used as bait destination address to bait malicious nodes to send a reply RREP message. Malicious nodes are thereby detected and prevented from participating in the routing operation, using a reverse tracing technique. In this setting, it is assumed that when a significant drop occurs in the packet delivery ratio, an alarm is sent by the destination node back to the source node to trigger the detection mechanism again.

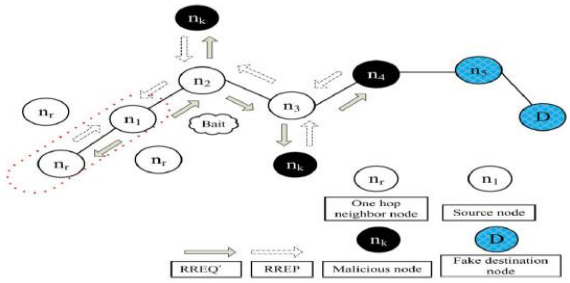


Figure 2 Existing System Architecture

DISADVANTAGES OF EXISTING SYSTEM:

- The lack of any infrastructure added with the dynamic topology feature of MANETs make these networks highly vulnerable to routing attacks such as blackhole and grayhole (known as variants of blackhole attacks).
- In this regard, the effectiveness of these approaches becomes weak when multiple malicious nodes collude together to initiate a collaborative attack, which may result to more devastating damages to the network.

IV. MODIFIED COOPERATIVE BAIT DISCOVERY SCHEME APPROACH

The proposed framework consist of amechanism [so-called Enhanced Cooperative bait detection scheme (ECBDS)] is presented that effectively detects the malicious nodes that attempt to launch collaborative Worm-hole attacks. In this scheme, the address of an adjacent node is used as bait destination address to bait malicious nodes to send a reply RREP message, and malicious nodes are detected using a reverse tracing technique. Any detected malicious node is kept in a Wormhole list so that all other nodes that participate to the routing of the message are alerted to stop communicating with any node in that list. Unlike previous works, the merit of ECBDS lies in the fact that it integrates the proactive and reactive defense architectures to achieve the before mentioned goal.

PROTECTED DATA TRANSMISSION

To make the data transmission secure after the detection of black hole attack, Key Distribution Center (KDC) provides key 'K' which is shared between source and the destination. Source generates theKEYusing number of hops (H_R)involved in the route and message sent time (T_S) .Using KEY, data is encrypted at the first level and generates Ciphertext1.In the second level, Ciphertext1 ,$T_S$and H_R are encrypted using K. In the second level before encrypting the $T_S$and H_R,theyshould be shuffled using some shuffling algorithm. The Ciphertext2 is sent to the destination. The destination makes use of K and decrypts the Ciphertext2.By making use of shuffling algorithm, destination obtains values of $T_S$and H_R..Using $T_S$and H_R, destination generates KEY.UsingKEY, Ciphertext1 is decrypted

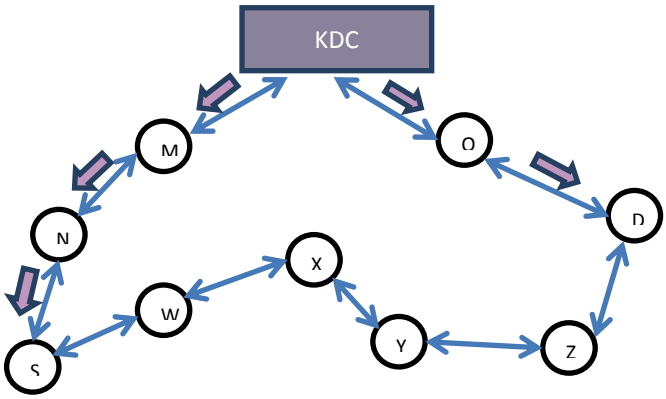
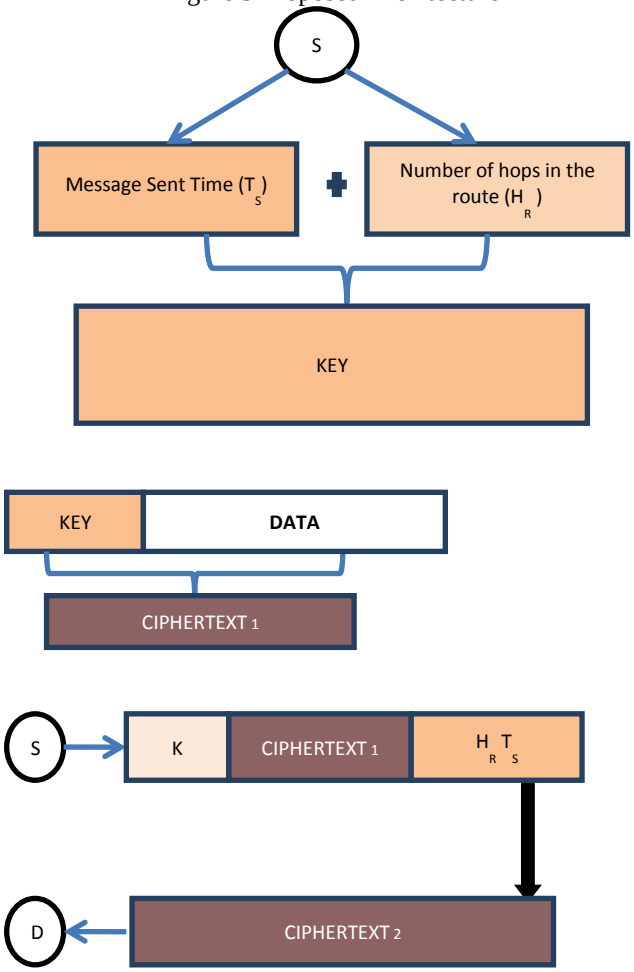


Figure 3 Proposed Architecture



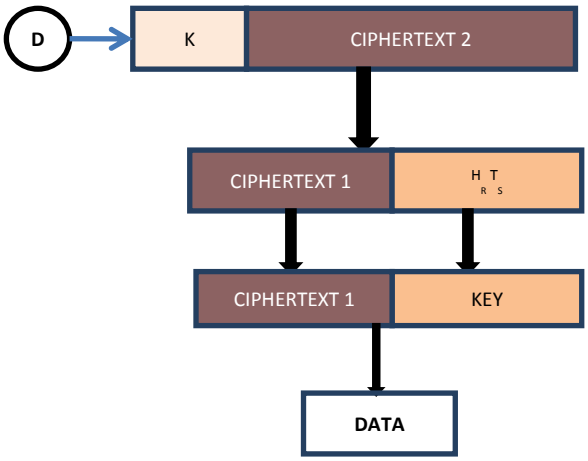


Figure 4 Flow Graph of KD2SA

MODULES

- Network Topology
- Dynamic Source Routing Algorithm
- Cooperative Bait Discovery Scheme

Network Topology

The sensor nodes are randomly distributed in a sensing field and due to that we are using mobile ad hoc network (MANET). This is the infrastructure less network and a node can move independently. In a MANET, each node not only works as a host and also acts as a router. We can find the communication range for all nodes. Every node communicates only within the range. If suppose any node is out of the range, that node will not communicate with all other nodes or simply drops the packets.

Dynamic Source Routing Algorithm(DSRA)

In this project, we are using dynamic source routing algorithm for routing. The DSRA involves two main processes: route discovery and route maintenance. The source node broadcast the RREQ through the network. If an intermediate node has the route information to the destination node in its cache, it will reply with a RREP to the source node. When destination receives the RREQ, it knows all the information about intermediate node. Then the destination will reply with RREP to the source node along with the routing information.

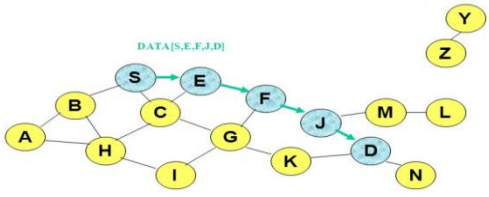


Figure 5 Dynamic source Routing

Cooperative Bait Discovery Scheme

We propose a detection scheme called Cooperative bait detection scheme (CBDS), which aims to detect the grayhole/collaborative blackhole attacks in MANET. In this scheme, the source node randomly selects the adjacent node is used as a bait destination address to bait malicious node to send a RREP message. We can find the malicious node in the routing operation by using the reverse tracing technique. If there is any malicious node detected in the routing, send the alert message or stop the communication with any node in that list. The CBDS scheme integrates the advantages of proactive detection in the initial stage and the reactive defense architecture to achieve the goal.

Performance Evaluation

In this section, we can evaluate the performance of simulation using the x-graph. We choose the three evaluation metrics: Packet delivery ratio – it is the ratio of the number of packet received at destination and number of packet sent by the source, End-to-End delay – the average time taken for a packet to be transmitted from the source to destination, Throughput – number of data received by the destination without any losses.

V. RESULTS AND DISCUSSIONS

In this section, we evaluate the performance of simulation using the x-graph. We choose the three evaluation metrics: Packet delivery ratio – it is the ratio of the number of packet received at destination and number of packet sent by the source, End-to-End delay – the average time taken for a packet to be transmitted from the source to destination, Throughput – number of data received by the destination without any losses.

This enhanced technique improves the performance of Packet delivery ratio, Throughput, End to end delay and Routing Overhead. These are all the parameters which bring up the performance better.

Simulation Parameters

PARAMETER	VALUES
Channel Type	Channel/WirelessChannel
Radio-Propagation Model	Propagation/TwoRayGround
Network Interface Type	Phy/WirelessPhy
MAC Type	Mac/802_11
Interface Queue Type	CMUPriQueue
Link Layer Type	LL
Antenna Model	Antenna/Omni Antenna
Max Packet In Ifq	50
Number Of Mobilenodes	33
Routing Protocol	DSR
X Dimension Of Topography	1100
Y Dimension Of Topography	1000
Time Of Simulation End	20.0 Sec

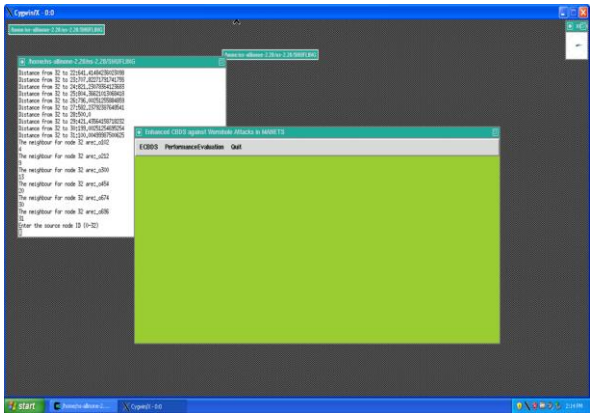


Figure 6 Node Selection

The source and the destination nodes are selected for the data packet transmission

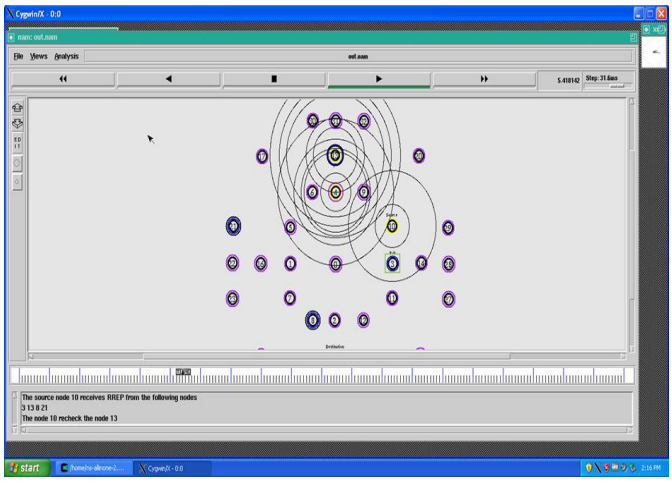


Figure 7 Packet Transmission

Source nodes 2 send packets to Destination node 15 by Neighbor nodes

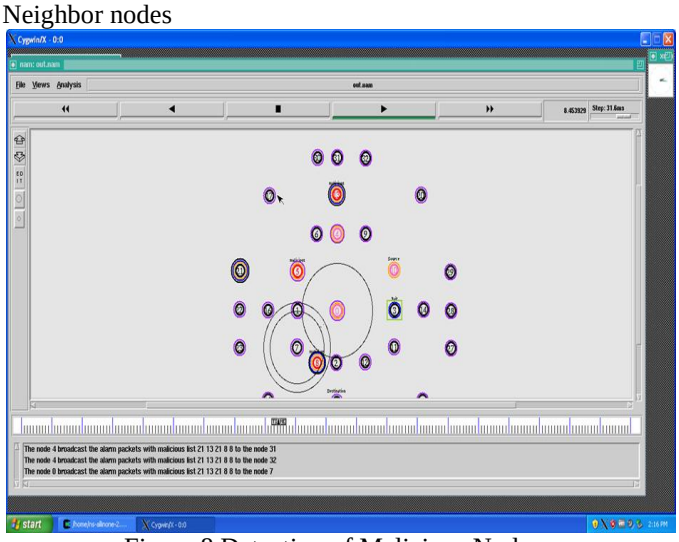


Figure 8 Detection of Malicious Nodes

The malicious nodes are detected by auditor nodes and packet transmission is stopped.

Figure 9 Packet Delivery Ratios.

Packet delivery ratio is the ratio of the number of packet received at destination and number of packet sent by the source. The greater value of packet delivery ratio means the better performance of network.

Figure 10 End To End Delay.

End-to-End delay is the average time taken for a packet to be transmitted from the source to destination. The lower value of end to end delay means the better performance of network.

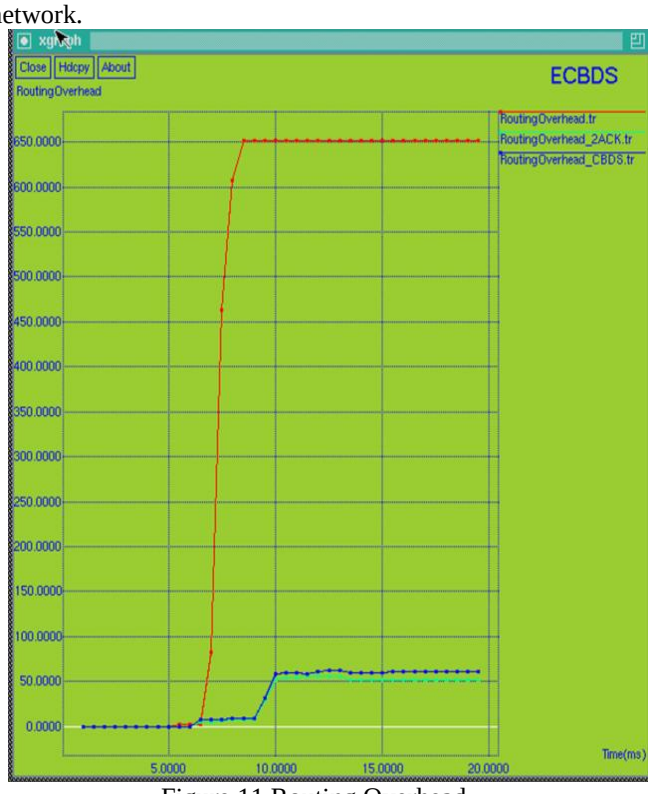


Figure 11 Routing Overhead.

Routing Overhead is the number of routing packets required by the routing protocol to construct and maintain the routes.

VI. CONCLUSION

In this project, we have proposed a mechanism (called the Enhanced CBDS) for detecting malicious nodes in MANETs under Wormhole attacks. Our simulation results revealed that the ECBDS outperforms the DSR, 2ACK, and CBDS schemes, chosen as benchmark schemes, in terms of routing overhead and packet delivery ratio and the feasibility of adjusting our ECBDS approach to address other types of collaborative attacks on MANETs and to investigate the integration of the ECBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against the malicious nodes.

REFERENCES

[1] JuRen, Yaoxue Zhang, Kuan Zhang and Xuemin "Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor Networks," IEEE Trans.Wireless Commun., vol. 15, pp. 3718-3731, May 2016.

[2] Bhargava, B, Wang.W and M. Linderman, "Defending against collaborative packet drop attacks on MANETs," in Proc. 28th IEEE Int. Symp. Reliable Distrib. Syst., New Delhi, India, Sep. 2009.

[3] Baadache.A and Belmehdi.A, "Avoiding blackhole and cooperative blackhole attacks in wireless ad hoc networks," Intl. J. Comput. Sci. Inf. Security, vol. 7, no. 1, 2010.

[4] Corson.S and. Macker.J , RFC 2501, Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, Jan. 1999. (Last retrieved March 18, 2013). [Online].Available:http://www.elook.org/computing /rfc/rfc2501.html

[5] Chang.C, Wang.Y, and H. Chao, "An efficientMesh-based core multicast routing protocol onMANETs," J. Internet Technol., vol. 8, no. 2, pp. 229– 239, Apr. 2007.

[6] Johnson.D and Maltz.D , "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[7] Kozma.W and Lazos.L, "REAct: resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. WiSec, 2009, pp. 103–110.

[8] Marti.S , Giuli T.J, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in Proc. 6th Annu. Intl. Conf. MobiCom, 2000, pp. 255–265.

[9] Pramod.D, Liu.K, Varshney.K, and K. Balakrishnan, "An Acknowledgement based approach for the detection of routing misbehavior in MANETs," IEEE Trans. Mobile Comput., vol. 6, no. 5, pp. 536–550, May 2007.

[10] Rubin.I, Behzad.A, R. Zhang, H. Luo, and E. Caballero, "TBONE: A mobile-backbone protocol for ad hoc wireless networks," in Proc. IEEE Aerosp. Conf., 2002, vol. 6, pp. 2727–2740.

[11] Ramaswamy.S, H. Fu, M. Sreekantaradhya, J. Dixon, and K. Nygard, "Prevention of cooperative blackhole attacks in wireless ad hoc networks," in Proc. Int. Conf. Wireless Netw., Jun. 2003, pp. 570–575.

